TELEPHONE (949) 364-1511
FAX (949) 363-7561
E-mail: mjfrank@deltanet.com
http://www.identitytheft.org

Mari J. Frank, Esq.
& Associates

28202 CABOT RD SUITE 215
LAGUNA NIGUEL, CALIFORNIA 92677-1248

- CIVIL LAW
- NEGOTIATIONS
- MEDIATIONS
- ARBITRATIONS
- PROFESSIONAL WORKSHOPS
- KEY NOTE SPEAKING

Identity Theft- The New Frontier:

Personal Protection Measures:

1. **Contact the three major credit-reporting agencies (CRA's).**
   - **Order your credit report from all three major credit-reporting agencies (CRA) at least two times a year.**

     Look for any debts you don't recognize and any credit inquiries that don't look familiar. For example, look closely for possible inquiries by a tenant screening company. That might mean someone has used your name to rent property—which could eventually lead to an eviction or other negative information being added to your report. If there are errors, make sure you immediately write to the CRA to have the items corrected or removed. If you see addresses where you have never lived and alias names that you don't recognize, immediately put a consumer (fraud) alert on your credit reports stating "Do not issue credit without first calling me at this phone number: _____." This won't stop negligent credit grantors from issuing fraudulent cards, but it will be a strong deterrent.

     To order your report, contact the following agencies:

     Equifax: http://www.equifax.com or phone 800-685-1111

     Experian: http://www.experian.com or phone 888-397-3742

     TransUnion: http://www.tuc.com or phone 800-888-4213

   - ***Immediately*** **correct all mistakes on your credit reports in writing**.

     Send a letter to the credit-reporting agency by certified mail, return receipt requested, identifying the mistakes item by item on a copy of the credit report. You should hear from the agency within 30 days (mark you calendar.) In a study performed in 1998, The U.S. Public Interest Research Group (USPIRG) found that 70 percent of credit reports have errors, and 29 percent are severe enough to keep you from obtaining credit**.**

     Your credit report is like a snapshot. By the time you request and receive it, it has probably changed because new information is being added all the time. The fact that it's good today doesn't mean it's going to be good tomorrow or the next day. So the moral is check it often, at least two times a year. It should be sent to you at no cost if you have been denied credit, are indigent, or if you are a victim of identity theft.

2. **Discarding and storing personal information.**

- **Buy and use a crosscut shredder.**

  For a small investment, you can purchase a crosscut shredder for all your important papers, *especially* pre-approved credit applications received in your name. Any paper you don't absolutely need to keep and provides private information should be destroyed.

- **Be careful of "Dumpster Divers."**

  Your trash can tell a lot about you—sometimes *too* much. Make sure that you don't throw away anything—an old tax bill, say, or credit-card receipts or brokerage statements—that someone could use to assume your identity.

- **Quiz every firm or organization—banks, brokerages, doctors' offices, accountants, lawyers and even your own employer—about what it does with your private information.**

  Many employers aren't sensitive to privacy issues. Thus, information handling often is unspeakably shoddy. Insist that they shred old data and have procedures in place to protect your current files.

- **Keep your financial records under lock and key.**

  Burglars may be more interested in your bank and credit card information than in your VCR. Furthermore, you'd be surprised at how many cases of identity theft involve a perpetrator known to the victim: a relative, client, roommate, cleaning service, tenant or someone else who has easy access to the victim's house and thus perhaps to his or her account numbers, SSN, or driver's license number. Don't leave or keep such information in your car, either.

3. Guarding your information in public places.

- **Carry as little information as possible in your wallet.**

  For starters, don't carry your Social Security card; you already know the number by now and you can take the original with you if you know you're going to be required to show it. Get rid of extra credit cards and other identifying data. In short, don't carry with you anything that you don't use or need.

- **Reduce the likelihood of your wallet or purse being stolen.**

  For starters, know exactly what's in it. Second, when in crowds, keep your wallet in a front pocket or keep your purse in front of you. You may prefer to keep your wallet in a pocket with a Velcro™ enclosure or put rubber bands around it so it won't slip out of your pocket so easily. You may also wish to subscribe to a credit-security service that registers all your credit cards and important documents. If you lose your purse or wallet or if it is stolen, notify each credit card company, or call your credit security service to cancel your cards. Then call the three major credit reporting agencies to place a fraud alert on your profile.

- **Memorize your Social Security number (SSN) and secret passwords.**

  You *can* do it! Don't carry your Social Security card in your wallet. Don't put this number or other important information on your computer without reliable encryption software.

- **Resist using your Social Security number for any kind of identification.**

  Unfortunately, more and more firms and organizations are using SSNs in careless ways—as student ID numbers, for company identification badges, and on Little League rosters. It'll take courage to resist this trend. Ask to have an alternative number to your SSN used for identification or enrollment. You will have to provide your SSN to anyone who employs you, the IRS, your accountant, your bank, your investments, broker and those who have a right to obtain your credit report, but you are not required to give it to others. There is no law that says that a company cannot ask for your Social Security number, so you need to explain your concern.

- **Don't put your address or license plate number on your key ring.**

  Doing so will merely point a thief to your home and car. If your keys have been stolen or lost and there is a way for a thief to find you, remember to change the locks on your house and automobile.

- **Be alert to "Shoulder Surfers."**

  Look around for suspicious people when you use your Automatic Teller Machine (ATM) or long-distance phone card. If someone's too close, ask him or her for privacy, or go to another machine. Be aware that high-tech cameras can be used to steal your numbers from afar. Use your hands and arms to shield the numbers you punch into the keypad. If your card gets stuck in the machine- watch out- it's a scam- immediately cancel the card.

- **Don't use ATM cards with Visa or MasterCard logo**

  This card number may be used online without a PIN number to make purchases. The money will come directly out of your account and you may never get it back since federal law does not protect those cards.

4. Dealing with credit cards.

- **Get credit cards with your picture on them.**

  Not all credit card issuers will do this, but some will. Shop around.

- **When you order new credit cards or your current ones are expiring, keep an eye on the calendar.**

  Be alert when a new card ought to be arriving. If it doesn't arrive when you expect it, call the credit card issuer immediately and find out if the card was sent. If it was sent more than 10 days ago, but you still haven't received it, cancel it at once.

- **Put passwords on all your financial accounts.**

  This may be bothersome and probably won't win you friends at the bank or with your creditors, but it's important.

  Carolyn, for example, was impersonated by a woman who worked at a medical office and stole the Identification (ID) information of 14 women patients. A year and a half later, Carolyn was still being hounded by collection agencies demanding she pay the imposter's bills. Our advice: Put a special password on all credit and bank accounts—and make it something other than your mother's maiden name, a pet's name, or the

name of someone in your family. It is a good idea to use a password that has a mixture of numbers and letters.

- **Cancel all credit cards that you haven't used in six months.**

  If you don't pare down your unused cards, you might as well be carrying around dynamite while waiting for a match. If you carry a little-used card, you are not likely to quickly notice if it's lost or stolen. Also, if the thief has your credit report, he or she has notice of an account that is ripe for extensive use. Thus, you're giving a thief a big head start.

- **Monitor all statements from every credit card.**

  If there's anything on the statement you don't recall buying, call the credit grantor to verify that the debt is truly yours. If it's not yours, cancel the card and get a new account number using a unique password. Make sure you put a fraud alert on that account.

- **Don't put your address, telephone number, or driver's license number on the credit card slip from restaurants or stores.**

  For ordering by mail you will need to complete address information on the order form. You do not need to write your driver's license or SSN on an order form.

- **Do not put your credit card account numbers on the Internet (except on a secure site with a company that you know), on the outside of envelopes, or on your checks.**

  Guard those numbers zealously. Never give out a credit card number unless you have a trusted business relationship with the company, and you call them, not vice versa. If you must shop on the Internet, use a secure browser that encrypts or scrambles purchase information, or place your order by telephone, fax, or mail.

- **If you think you've misplaced or lost a credit card, assume the worst.**

  Call the issuing bank *immediately*. As Allan Troisclair, a former FBI agent and former Vice President of Fraud Control at Visa USA, puts it: "If you think you lost it [your credit card] around the house, don't spend three or four days looking for it. The bad guys use it up in two days. So call immediately, don't take the chance." It costs the banks about $125 to issue a new card, he said, "But they'd rather do that than have a couple hundred thousand dollars of fraud on your account."

- **Keep a list of all your credit cards and bank accounts.**

  Include the account numbers, expiration dates, and phone numbers of the issuers' customer service departments. Update the list as needed and keep it in a secure place (not the hard drive of your computer) so you can quickly contact your creditors if your cards are lost or stolen. Do not keep this information on your computer especially if you use the Internet.

  Jeff Levy, Computer Expert and host of the syndicated talk radio show (in Los Angeles, based on KFI): "Jeff Levy On Computers" advises: "Avoid storing your personal information on your computer. Things that require your name and your social security information should never be kept on your hard drive. If you must supply that information, keep it on a floppy disk and keep that disk under constant lock and key.

Quicken, Microsoft Money, and other programs that track our financial information all allow us to store data on floppy disks, not on the hard drive."

For Internet users: Create a list of all your credit card companies (don't list the account numbers) with the their toll-free numbers. Save it in draft in a file folder with a web-based e-mail account like Yahoo. This will provide you instant access to your credit card companies to cancel your accounts in the event of loss or theft of your wallet, even when you are away from home.

5. **Protecting your checks.**

   - **Don't print your Social Security number (SSN) on your checks.**

     And don't allow merchants to write it on the checks, either. Retailers don't need it—thieves *do*. Also, don't print your SSN on your business cards, address labels, invoices, or other identifying information. Try to convince your employer to do the same.

   - **Don't put your telephone number on your checks, either**.

     If a merchant asks you for it, you can decide to write it on if you wish.

   - **When you order new checks, have them delivered to your local bank branch, not to your home.**

     Boxes of blank checks are readily recognizable and an easy target for mailbox thieves.

6. **Protecting information by phone.**

   - **Never give out any personal information over the phone to someone you don't know.**

     If someone tells you he or she represents a credit grantor of yours, call the person at a telephone number that you know is the *true* number and ask for that person. Even then, provide only information that you believe is absolutely necessary.

   - **Never give confidential or financial information on a cellular or cordless phone.**

     High tech scanners are able to listen in on your conversations when you least expect it. Your wireless transmissions are not secure.

7. **Protecting your mail.**

   - **Do not put checks in the mail from your home mailbox.**

     When you pay your bills, make the effort to walk down the street to a mailbox or to drive to the post office. If you leave them as outgoing mail for the letter carrier, you'll create an easy target for a thief who can probably learn a great deal about you from that handful of envelopes. Also, it's not hard for a crook to steal a check, acid wash the name of the recipient, and make himself or herself the payee. We suggest you use the "Pay By Phone" service from your bank. There are no checks sent by mail, and the bank's electronic payment will show up on your statement.

   - **Get a post office box or a locked residential mailbox**.

     Theft of mail is so easy—and so potentially ruinous to your identity. This is a simple precaution that pays big dividends in peace of mind.

   - **Use "Pay By Phone" from your bank.**

This way, you don't have to use checks to pay bills. Your bank will automatically pay as you request and your statement will reflect payment.

8. Blocking your name from marketing lists.

- **Opt out of unsolicited credit and insurance offers.**

  Choose to exclude your name from credit bureau lists for unsolicited (*"You've been pre-approved!"*) credit offers. Tell them you don't want your credit report used for marketing purposes. This will limit the number of pre-approved offers of credit that you receive. These, when tossed into the garbage, are potential targets of identity thieves, who use them to order credit cards in your name.

  "The best way to avoid becoming a victim," says Ed Mierzwnski, consumer program director of the USPIRG, "is to block your name from being marketed to." The best way to reduce, if not eliminate, being marketed to is to sign up for the Direct Marketing Association's (DMA) Mail Preference Service and its Telephone Preference Service.

  Doing so should delete your name from lists used by nationwide marketers, though to stop locally generated junk mail, you'll need to contact local merchants yourself. To stop other junk mail, write to your banks and credit card companies and tell them not to sell your name.

  You can write the DMA at:

  Direct Marking Association
  Mail Preference Service
  Box 9008
  Farmingdale, NY 11735
  or
  Direct Marketing Association
  Telephone Preference Service
  Box 9014
  Farmingdale, NY 11735
  http://www.the-dma.org

  Creditors and insurers are legally allowed to use credit reports to generate such junk mail; banks also are allowed to share your credit report with their "affiliates," such as a mutual-fund company. However, the law also says that all such offers must include a toll-free number for you to call if you want your name and address removed from future lists. You should do this.

  The number to call to "opt out" at the big three credit-reporting agencies is:

  1-888-5-OPTOUT

  (1-888-567-8688)

  Banks and credit card companies making offers through their affiliates are not required to have an 800 number for opt outs, but they must send you a one-time offer to opt out. Write to your credit card companies (return receipt requested) and ask them to remove

you from their promotional lists. Ask them not to sell your name, creditworthiness, or spending habits to any other company without your permission.

Many professional organizations sell their member lists for marketing purposes. Write your professional associations and ask them to stop selling your name to other entities.

- **Notify your state's department of motor vehicles that you don't want your personal data sold.**

  Illinois prisoners were data processing the personal information for vehicle licenses to save money for the state. These criminals armed with private information had many opportunities to commit identity theft. Find out how your personal information is entered into your state's databases and complain where appropriate. Ask to have your name removed from lists that are sold to marketers. Some states still use the social security number for the driver's license number. If this is the case in your state, ask for an alternative number.

- **Don't participate in phone surveys, marketing surveys, or contests, and don't fill in personal information on warranty cards**.

  Jane, a single mom, completed an in depth marketing survey on a warranty card. It included her social security card and extensive information about her income, place of work, and so forth. A few months later she found out her identity was stolen by someone who had seen the marketing survey.

  Heed her advice: Throw those surveys away!

9. Internet protection.

- **Strengthen your computer's log-in security**

  Remove or encrypt private confidential files with your personal information. Your passwords are the keys to unlock the door to your identity — guard them. Don't be lazy and store them on your computer; type them each time you access a particular site. Learn how to browse the Internet and send e-mail messages without leaving a trail to keep from being an easy target. (See http://www.pcworld.com for ideas to protect your privacy when using the computer.)

- **Install computer hardware (routers) or software that acts as a firewall to protect your financial and personal data on your hard drive.**

  If you use a modem or are connected to the Internet or a network, you need to block access to your hard drive.

- **Tell your Internet service provider that your personal data is not for sale.**

  Find out the company's privacy policy and inform the service that any information you provide is not for sale and that you will hold the service accountable if it fails to maintain your privacy.

- **Don't register when visiting websites on the Internet unless you are comfortable with their privacy policies.**

  Many websites ask for a great deal of information about your personal life. Before you sign a "guest book" find out the privacy policy. How is the information stored and will it be sold? The web page owners have the ability to collect little pieces of

data about you and store them in "cookie" files on your computer, which they can also share with other website owners. Ask websites what they do with your personal data before you give too much information. The more information someone can access about you, the easier it is to assume your identity.

- **Erase your name from Internet online directories.**

  It is easy to find your name, address, and e-mail address on the web. Remove this information from the major on-line directories:

  http://www.Four11.com Send e-mail to support@Four11.com. Send your name and full e-mail address and ask to be removed from the listing.

  http://www.InfoSpace.com Find yourself in the white pages and go to the bottom of the page and choose the option to remove yourself.

  http://www.Switchboard.com Click Create/Modify Listing. Then click "Get a password". When your password appears, log in. Click "Modify Main Listing." "Scroll to Privacy Options" and hide your listing.

  http://www.whowhere.com Click "e-mail Directory" and ask to be removed.

- **Opt out of "look-up" companies' databases.**

  There are numerous information companies. Here is a major company you can call to get your name and personal information off their list:

  Lexis-Nexis: 800-227-9597

- **Don't display your personal or family information on the Internet.**

  Creating your own homepage or family tree website with identifying information and photos of your family gives an imposter lots of data with which to create his or her new identity.

- **Check yourself out on the web and delete or correct information.**

  Search people finders, genealogical sites, public records, and governmental sites. Check out your name with multiple search engines. Here are some sites that have background information about consumers. You may be surprised at what you find:

  http://www.knowx.com Uses Information America Database.

  http://www.informus.com Conducts public record searches.

  http://www.advsearch.com Provides background checking services.

  http://www.digdirt.com Provides information access to 325 billion records.

  http://www.peoplewise.com Provides instant background checks for employers.

- **Don't give out your Internet account password to anyone.**

  If you do, you may find unexpected charges on your bill and lots of other problems.

- **Don't trust people you meet on line.**

  You may find the love of your life or an evil-minded criminal online. Don't give out personal information to people you do not know or have not met (or haven't checked

out.) Use extreme caution in entering chat rooms as well. Remain anonymous and use a nickname for your screen name.

- **Teach your children never to give personal information on the Internet about any family member.**

  Kids are especially vulnerable and innocent. Explain the dangers of giving out personal information about your family. Install software filters that will help protect your children from websites that could be harmful. Make up strict rules for using the Internet.

Workplace Identity Theft Precautions.

Here is an example of how your business can be stolen by an identity thief:

Dr. George is a successful ophthalmologist. Without his knowledge, one of his part-time bookkeepers opened a bank account using Dr. George's name and deposited checks that were made out to the doctor. The imposter then ordered $10,000 worth of eyeglasses and thousands of dollars worth of equipment for the office he rented as Dr. George. For over a year, the imposter continued to work for Dr. George, diverted checks into the fraudulent account, and also ran a business under the name of Dr. George. This identity theft was revealed when Dr. George found out his credit was ruined because the imposter did not pay his bills.

Corporations and business owners need to protect the privacy and identity of their businesses, the people who work for them, their vendors, and their customers. So whether you are an employer, employee, or a customer, you need to be aware of how to take responsibility for protecting your private information in commerce. If you are an employee or do business with a company you should ask questions to ascertain how your personal information is used and secured.

We will address the issue of privacy and identity theft protection on two levels: the first from the perspective of inside customers (business staff) and second for dealing with outside customers (consumers.) The personal guidelines apply to the consumer precautions as well. Here are some tips that will guide you.

Protection Measures for Corporate and Business Owners and Employees.

Here is a sad example of identity theft caused by an insider:

Paul, who worked in the Human Resources Department, stayed late one evening. He made copies of the personal information of one of the high-paid executives. He sold that information to someone who stole the executive's identity and caused him years of anguish in cleaning up the financial mess.

Obviously, we *cannot g*ive you a failsafe way of protecting yourself and your workplace associates because we cannot control human behavior. Additionally, savvy imposters create new technologies and tricks every day. We can assure you, however, that these steps will create a much safer environment, give you greater peace of mind, and provide more control over your confidential information.

1. **Have strict audit procedures and periodic check-review policies. Make sure your company does criminal and civil background checks before hiring employees ¾ even if they're part-time.**

   Most people are honest and trusting. Unfortunately, we all need to temper our trust with caution and inquiry. Your company could be held legally liable for negligent hiring if a victim of identity theft can trace the crime back to one of your employees who had a criminal background that you failed to detect.

2. **Keep all personal information about all employees in locked cabinets. Have data security procedures for those who have access to the files.**

   Only specific persons with up-to-date training should be assigned to data security. Sensitive files should be segregated. There should be procedures to prevent ex-employees from gaining access to paper and computer files.

3. **Limit the use of personal identifiers.**

   The use of a Social Security number for identification and record keeping exposes everyone to the risk of identity theft. Use an alternative number for all employees and customers. Don't display personal data on documents that are widely seen by others such as on mailing labels. Access codes should not be birth dates or Social Security numbers.

4. **All personal and confidential information on computers should be encrypted.**

   The organization should regularly conduct "systems-penetration tests" to determine if all systems are "hacker proof". For electronic transmission (over networks and the Internet), encryption should be used for all confidential information about employees, customers, and business trade secrets. Extra precautions should be taken to prevent industrial espionage and business identity theft.

5. **Put photos on business cards for identification. (It's also good marketing.)**

   One imposter stole an attorney's business cards from the receptionist's desk. The imposter used the business cards along with other false identification to steal thousands of dollars in credit and parade as a lawyer, ruining the reputation of the victim. That attorney recommends using photo business cards.

6. **Have a proven method of disposing of personal information.**

   Industrial shredders should be used at large offices. Consider providing a personal crosscut shredder at each workstation or at least locked garbage bins. For companies that outsource the shredding of documents, care should be taken to keep the material locked up until pickup. The shredding company should have strict security procedures in place. Shredding software should be used to delete confidential information from computer files. When disposing of computers, diskettes, magnetic tapes, and hard drives, erase them with an "initialize process" or a wipe function, or physically destroy them.

7. **Train designated staff about security procedures in sending sensitive personal information by fax.**

   Only authorized persons should send sensitive documents. All faxes should have a confidential cover sheet (prohibiting re-disclosure), and the fax number should be double-

checked before sending. You should call the recipient before sending and acknowledge receipt afterward.

8. **No one should leave or send personal, confidential, or sensitive information by voice-mail, cell phones, pagers, answering machines, or e-mail at any time.**

   None of these transmissions is private or secure. Under current case law, sending your own (or anyone else's information) at work by these devices is subject to review by the employer and possibly others**.** In fact it could be used for legal purposes.

9. **Designated, secure printers and copiers should be used for confidential information.**

   Care must be taken to not direct confidential information to the wrong printer. Draft copies should be shredded immediately**.**

10. **Have a written privacy protection policy that covers all persons within the organization and applies to dealings with persons outside the organization.**

    All employees and even your board of trustees should be trained in the company's security measures and privacy protection policies. You should review these policies and update them regularly followed by retraining. Even temporary, part-time, and independent consultants should be made subject to the written policies. For the many employees working at home or away from the office on trips, there should be special guidelines for information handling offsite.

Protective Measures for Your Customers and Clients.

American consumers are becoming increasingly concerned about their lack of control over their personal information and decreased privacy. A recent *Business Week Harris Poll* found that 53 percent of the respondents believe that laws should be passed to specify how personal information could be collected and used. Your customers and clients trust you and rely on you to protect their personal information. Your company may have legal exposure for failing to protect someone's privacy if damages result from your failure to act in a responsible manner. Additionally, companies in our nation may be precluded from doing business with other countries that have stricter information-protection policies.

Currently the European Union has developed *The European Data Protection Directive*, which went into effect in October 1998. Countries wishing to do electronic commerce and share databases with European countries must be in compliance within the privacy policies. The directions state that data can be collected only if an individual consents and is told how it will be used and if there is a right to access to correct or erase the information. The United States is far from being in compliance. The voluntary measures negotiated by the Federal Trade Commission do not comply. Presently, consumers in the United States have no idea what information is being sold about them by direct marketing companies, large corporations, businesses, or governmental agencies. Our country has no privacy commission and few laws dealing with control of our information.

Institute policies and procedures to give consumers a right to determine when, how, and to what extent their personal information is communicated to others.

We encourage government and private industry to develop workable procedures for securing our information. The following list of fair information guidelines is adapted from policies originally developed by the Organization for Economic Cooperation and Development and most recently by the Federal Trade Commission in the June, 1998 Report To Congress: "Privacy Online." These are forming the basis of privacy laws and business practices, and should be instituted globally to protect us in the information age:

1. **Provide consumers with notice of your company's information handling policies.**

   Before the information is given, consumers should be provided *written* notice of: the identification of the entity collecting the data; the proposed uses; who will receive the information; how it will be collected, whether it is voluntary; the consequences of refusal to provide the data; and the degree to which the data is ensured as to confidentiality and accuracy.

2. **Clearly define the specific use of the information.**

   The consumer should be told why the information is being collected at the time it is gathered. That information should not be used for any other purpose or provided to anyone else without prior permission of the individual consumer.

3. **Give consumers options as to how to participate in the collection of their information.**

   Consumers should have the right to make choices as to how their information is used. Consent to all uses should be clear, easy, and detailed.

4. **Provide consumers an opportunity to inspect their information.**

   Consumers should have a right to easily access, inspect, and correct errors (and delete if appropriate) concerning his or her personal information.

5. **Develop quality controls, which include strict security measures.**

   Collected information should be accurate, complete, timely, and relevant for the defined purpose. It should be protected from inappropriate access or corruption and safeguarded against loss or destruction.

6. **Implement standards of accountability, enforcement, and redress.**

   Every business or governmental agency must be held accountable for complying with reasonable privacy procedures. Entities should conduct their own information protection audits, and provide regular information protection training for their employees. There should be effective fair information use regulations enforced by a governmental entity like the Federal Trade Commission. The creation of private civil remedies (including punitive damages and class action lawsuits) for consumers harmed by misuse of their personal information would provide incentive for entities to comply with the fair information practices. Without legal enforcement including a possibility of sanctions, compliance is unlikely.

In addition to the privacy guidelines above, consider the following:

1. **Display a privacy protection policy in your literature and on your company's website.**

   Make sure all employees are aware of the policy and can assist clients. The literature and website should afford customers and clients an opportunity to communicate concerns and complaints regarding the use of their information.

2. **Train your employees about identity theft prevention and survival.**

   When an identity theft victim contacts your company (due to fraud in connection with your organization) make sure your customer service and fraud departments are well trained and know how to advise victims. By helping the victim to clear his or her record and by demonstrating your cooperation with law enforcement, your company may be ordered restitution, and you will limit your legal exposure as to the victim.

3. **Don't share, sell, or transmit data about your customers without their permission.**

   Guarding that information will also limit your legal exposure if that information subjects your customers to identity theft.

4. **Make sure that any person you are dealing with is truly the customer he or she claims to be.**

   The estimated corporate losses from computer crime in 1997 were $136 million. The annual losses from credit card fraud are over $900 million. When a customer pays by credit and tells you he or she has moved, verify the change of address with a phone call to the previous phone number and/or send a note to the former address to see if a move was really made. Carefully scrutinize suspicious documents. If you are a credit grantor, never issue instant credit without at least three pieces of identification, including a photo ID with an address (compare it to the address on the credit report).

5. **Remain positive, persistent, patient, and service oriented.**

   As should be clear now, you must be proactive in protecting yourself and your customers when dealing with information commerce. Governmental institutions, banks, credit grantors, and small businesses are made up of people just like us, so explain to them your concerns about privacy protection and identity theft. If customers are fearful about providing information, truthfully apprise them of your privacy policies and how your company will ensure their information. Be honest, and don't encourage a consumer to divulge unnecessary information that makes him or her feel uncomfortable. You need to be sensitive to privacy and identity theft protection.

6. **Ask your state and federal legislators for stronger privacy protection.**

   The anti-privacy forces are powerful, and voices for greater individual protections are few. You can help by voicing your concerns. Privacy advocate Robert Ellis Smith recommends calling your congressperson and sitting down with his or her staff, educating them about what is going on, and pointing out to them the "absolute epidemic" of identity theft. "Try to come armed with statistics and then give your personal account," Smith says. "And it

may not lead to legislation, today or tomorrow, but that person will have gotten an education, and it will certainly have an impact in the years to come."

You may join advocacy or lobbying groups to make your concerns known. Join USPIRG or your local state PIRG, both of which lobby for consumer legislation to protect you. Find them on the Internet at **http://www.pirg.org.** Also visit the Privacy Rights Clearinghouse at **http://www.identitytheft.org,** the Electronic Privacy Information Center **http://www.epic.org,** Mari Frank's Identity Theft Prevention and Survival website at **http://www.identitytheft.org** and the Federal Trade Commission's web site on Identity Theft at **http://www.consumer.gov/idtheft**. As one person alone, you may not have the power to effect change, so cooperate and support consumer groups, that protect your identity and the identity of your friends and family. Together, we can make a difference.

The above is adapted from an excerpt from Mari Frank's book "**From Victim to Victor**" (Porpoise Press, 1998, 2000) which is included in "**The Identity Theft Survival Kit**" by Mari Frank (Porpoise Press, 1998, 2000).